

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-098461  
(43)Date of publication of application : 09.04.1999

(51)Int.Cl. H04N 5/92  
G06F 12/14  
G09C 5/00  
H04N 1/40  
H04N 1/44  
H04N 5/91

(21)Application number : 09-251185  
(22)Date of filing : 16.09.1997

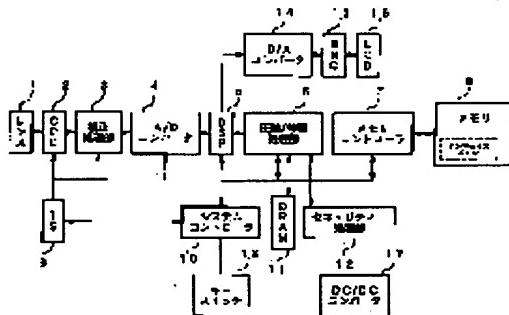
(71)Applicant : SHINKO ELECTRIC CO LTD  
(72)Inventor : SUGIYAMA HAYAMI

**(54) DIGITAL IMAGE RECORDER**

**(57)Abstract:**

**PROBLEM TO BE SOLVED:** To check a forged image by using an inverse function of a unidirectional function employing a decoding key so as to encrypt index image data generated resulting from sampling received image data.

**SOLUTION:** Input data are given to a DSP 5, where the signal are converted into R, G, JB data corresponding to each pixel and the converted data are given to a compression/expansion processing section 6, in which the data are compressed and the compressed data are interleaved to produce index image data. Then a security processing section 12 applies an inverse function to a unidirectional function to the index image data to encrypt the data by means of decoding key data resulting in producing the encrypted index data. The encrypted index data with security are decoded as encrypted index data by using a unidirectional function and a public key data given in advance. Then the presence of forgery is discriminated by comparing the decoded data with original index image data.



## **LEGAL STATUS**

[Date of request for examination] 22.01.2001

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁 (JP)

## (12) 公開特許公報 (A)

(11)特許出願公開番号

特開平11-98461

(43)公開日 平成11年(1999)4月9日

(51) Int.Cl.<sup>6</sup>  
 H 04 N 5/92  
 G 06 F 12/14  
 G 09 C 5/00  
 H 04 N 1/40  
 1/44

識別記号  
 3 1 0

F I  
 H 04 N 5/92  
 G 06 F 12/14  
 G 09 C 5/00  
 H 04 N 1/44  
 1/40

H  
3 1 0 Z

Z

審査請求 未請求 請求項の数 9 O L (全 7 頁) 最終頁に統く

(21)出願番号 特願平9-251185

(22)出願日 平成9年(1997)9月16日

(71)出願人 000002059  
神鋼電機株式会社  
東京都江東区東陽七丁目2番14号(72)発明者 杉山 早実  
三重県伊勢市竹ヶ鼻町100番地 神鋼電機  
株式会社伊勢事業所内

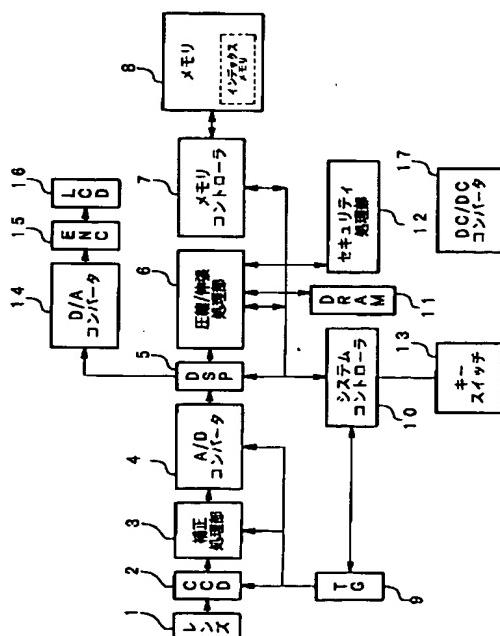
(74)代理人 弁理士 志賀 正武 (外11名)

(54)【発明の名称】 デジタル画像記録装置

## (57)【要約】

【課題】 改ざんが行われたインデックス画像のチェックができるデジタル画像記録装置と、さらに画像そのものにセキュリティをかけ改ざん不能にすることができるデジタル画像記録装置の提供。

【解決手段】 画像データ21をサンプリングしたインデックス画像データに対して電子印鑑と同様の原理により、一方向関数の逆関数を使って復号鍵データによりセキュリティをかけ、画像データを暗号化し、このセキュリティをかけられた画像データは、一方向関数を使って、予め与えられている公開鍵25データを用いることにより暗号化インデックスデータ24を復元し、原インデックスデータとの比較により改ざんの有無をチェックすることができる。さらに、画像データそのものに同様のセキュリティをかけ暗号化圧縮画像データとし、改ざん不能にする。



## 【特許請求の範囲】

【請求項1】 デジタル画像記録装置が取り込んだ画像データをデータ処理して記憶する記憶手段と、該記憶手段の記憶データを記録する記録媒体と、該記録媒体からデータを読み出し、このデータの編集を行うためのパソコンと、前記編集後の画像データを印刷するプリンタまたは前記画像データをデジタルデータとして記録、保存する保存媒体とからなる画像処理システムにおいて、前記デジタル画像記録装置が取り込んだ画像データをサンプリングしてインデックス画像データを作成し、該インデックス画像データに対し電子印鑑と同様の原理により復号鍵による一方向関数の逆関数を用いて暗号化することを特徴とするデジタル画像記録装置。

【請求項2】 前記記録、保存されるデータは下記5種類のデータがセットデータとして記録、保存されることを特徴とする請求項1に記載のデジタル画像記録装置。

- (1) 圧縮された画像データ
- (2) 画像に対応した個別情報データ
- (3) 復号鍵によって暗号化されたインデックス画像データ
- (4) 暗号化されたインデックス画像データを復元するための公開鍵
- (5) 圧縮画像データからインデックス画像データを作成する作成方法

【請求項3】 前記画像データ改ざんの有無を判定するために、

前記公開鍵による一方向関数を使って前記暗号化されたインデックス画像を復元することを特徴とする請求項1または2に記載のデジタル画像記録装置。

【請求項4】 前記画像データ改ざんの有無の判定するために、

前記画像データからインデックス画像を作成し、この画像と前記公開鍵による一方向関数を使ってインデックス画像データを復元することを特徴とする請求項1または2に記載のデジタル画像記録装置。

【請求項5】 デジタル画像記録装置が取り込んだ画像データをデータ処理して記憶する記憶手段と、該記憶手段の記憶データを記録する記録媒体と、該記録媒体からデータを読み出し、このデータの編集を行うためのパソコンと、前記編集後の画像データを印刷するプリンタまたは前記画像データをデジタルデータとして記録、保存する保存媒体とからなる画像処理システムにおいて、前記デジタル画像記録装置が取り込んだ画像データに対し、電子印鑑と同様の原理により復号鍵による一方向関数の逆関数を用いて暗号化することを特徴とするデジタル画像記録装置。

【請求項6】 前記記録、保存されるデータは下記3種類のデータがセットデータとして記録、保存されることを特徴とする請求項5に記載のデジタル画像記録装置。

- (1) 暗号化された圧縮画像データ

## (2) 画像に対応した個別情報データ

(3) 暗号化された圧縮画像データを復元するための公開鍵

【請求項7】 前記復号鍵のデータは読み出し不可能な不揮発メモリ等に記録されることを特徴とする請求項1ないし6のいずれかに記載のデジタル画像記録装置。

【請求項8】 前記復号鍵のデータは個々のデジタル画像記録装置に固有のデータであることを特徴とする請求項7に記載のデジタル画像記録装置。

10 【請求項9】 前記復号鍵のデータは複数台のデジタル画像記録装置に共通のデータであることを特徴とする請求項7に記載のデジタル画像記録装置。

## 【発明の詳細な説明】

## 【0001】

15 【発明の属する技術分野】 この発明は、デジタル画像記録装置の画像処理のうち、特に画像セキュリティシステムに関する。

## 【0002】

【従来の技術】 従来、工事写真等、証拠を証明する目的で使用される写真は、専ら銀塩写真が用いられてきた。しかし、CCDイメージセンサを用いたデジタルカメラの普及につれて、業務効率改善の一環としてこのデジタルカメラが採用されるようになりつつある。

20 【0003】 デジタルカメラを使った写真システムを図3に示す。この写真システムの概略は、まず、デジタルカメラ31で目的の写真を撮影すると、この画像は、CCDイメージセンサに取り込まれ、相関二重サンプリング、ガンマ補正、自動ホワイトバランスの各補正処理が行われた後、このアナログ信号はデジタル値に変換処理される。さらに、デジタル信号プロセッサ(DSP)によって各ピクセルに対応したR、G、Bデータに変換され、画像データの圧縮が行われた後、メモリに保存される。このメモリには画像データの他、撮影条件、日付、画像ファイル記号などの付随情報が記録される。

25 35 【0004】 次に、パソコン37に画像を転送する方法には二通りの手段があり、その第1は、メモリカード34など何らかのメモリにデータを保存し、パソコン37に読み込む方法であり、第2の方法は、デジタルカメラ31本体のインターフェース33とパソコン37のインターフェース36とを接続し、データを伝送する方法である。さらに、パソコン37にインストールされているアルバム編集用ソフト41によって、工事アルバムに編集する。編集結果はプリンタ39によりプリント出力し、アルバムとしてバインドされる。また、この編集結果はCDR40によってCD-ROMに仕上げられ、デジタルデータとして記録、保存される。

## 【0005】

【発明が解決しようとする課題】 ところが上述の方法ではデータ転送、画像編集の段階で画像を改ざんしようとすれば、容易に改ざんすることができ、証拠写真として

の信頼性に欠けるという問題点の解決が課題となっていた。本発明はこのような背景の下になされたもので、改ざんが行われた画像のチェックができるデジタル画像記録装置の画像セキュリティシステムと、さらに画像そのものにセキュリティをかけ改ざん不能にすることができるデジタル画像記録装置の画像セキュリティシステムとを提供することを目的とする。

## 【0006】

【課題を解決するための手段】請求項1に記載の発明は、デジタル画像記録装置が取り込んだ画像データをデータ処理して記憶する記憶手段と、該記憶手段の記憶データを記録する記録媒体と、該記録媒体からデータを読み出し、このデータの編集を行うためのパソコンと、前記編集後の画像データを印刷するプリンタまたは前記画像データをデジタルデータとして記録、保存する保存媒体とからなる画像処理システムにおいて、前記デジタル画像記録装置が取り込んだ画像データをサンプリングしてインデックス画像データを作成し、該インデックス画像データに対し電子印鑑と同様の原理により復号鍵による一方向関数の逆関数を用いて暗号化することを特徴とするデジタル画像記録装置を提供する。

【0007】請求項2に記載の発明は、前記記録、保存されるデータが下記5種類のデータがセットデータとして記録、保存されることを特徴とする請求項1に記載のデジタル画像記録装置を提供する。

- (1) 圧縮された画像データ
- (2) 画像に対応した個別情報データ
- (3) 復号鍵によって暗号化されたインデックス画像データ
- (4) 暗号化されたインデックス画像データを復元するための公開鍵
- (5) 圧縮画像データからインデックス画像データを作成する作成方法

【0008】請求項3に記載の発明は、前記画像データ改ざんの有無を判定するために、前記公開鍵による一方向関数を使って前記暗号化されたインデックス画像を復元することを特徴とする請求項1または2に記載のデジタル画像記録装置を提供する。

【0009】請求項4に記載の発明は、前記画像データ改ざんの有無の判定するために、前記画像データからインデックス画像を作成し、この画像と前記公開鍵による一方向関数を使ってインデックス画像データを復元することを特徴とする請求項1または2に記載のデジタル画像記録装置を提供する。

【0010】請求項5に記載の発明は、デジタル画像記録装置が取り込んだ画像データをデータ処理して記憶する記憶手段と、該記憶手段の記憶データを記録する記録媒体と、該記録媒体からデータを読み出し、このデータの編集を行うためのパソコンと、前記編集後の画像データを印刷するプリンタまたは前記画像データをデジタル

データとして記録、保存する保存媒体とからなる画像処理システムにおいて、前記デジタル画像記録装置が取り込んだ画像データに対し、電子印鑑と同様の原理により復号鍵による一方向関数の逆関数を用いて暗号化することを特徴とするデジタル画像記録装置を提供する。

【0011】請求項6に記載の発明は、前記記録、保存されるデータが下記3種類のデータがセットデータとして記録、保存されることを特徴とする請求項5に記載のデジタル画像記録装置を提供する。

- 10 (1) 暗号化された圧縮画像データ
- (2) 画像に対応した個別情報データ
- (3) 暗号化された圧縮画像データを復元するための公開鍵

【0012】請求項7に記載の発明は、前記復号鍵のデータが読み出し不可能な不揮発メモリ等に記録されることを特徴とする請求項1ないし6のいずれかに記載のデジタル画像記録装置を提供する。

【0013】請求項8に記載の発明は、前記復号鍵のデータが個々のデジタル画像記録装置に固有のデータであることを特徴とする請求項7に記載のデジタル画像記録装置を提供する。

【0014】請求項9に記載の発明は、前記復号鍵のデータが複数台のデジタル画像記録装置に共通のデータであることを特徴とする請求項7に記載のデジタル画像記録装置を提供する。

【0015】  
【発明の実施の形態】以下、この発明の一実施形態について図を参照しながら説明する。なお、デジタルカメラを使った写真システムの構成は「従来の技術」の項で説明した図3と同一である。図1はこの発明の一実施形態による画像セキュリティシステムを備えたデジタルカメラの構成を示すブロック図であり、図2は画像セキュリティシステムによる電子ファイル構造のイメージ図である。

【0016】図1において、符号1はデジタルカメラ31のレンズ、符号2はCCDイメージセンサ、符号3は相間二重サンプリング(CDS)、ガンマ補正(γ)、自動ホワイトバランス(AWB)処理を行う補正処理部、符号4はアナログ信号をデジタル値に変換するA/Dコンバータ、符号5はデータを各ピクセルに対応したR、G、Bデータに変換するデジタル信号プロセッサ(DSP)である。

【0017】符号6は画像データの圧縮/伸張処理部であり、メモリ8に格納する場合は例えば、JPEG方式などによりデータの圧縮を行い、メモリ8からデータを読み出しLCDモニタ16に表示する場合はデータの伸張を行う。符号7はメモリコントローラであり、画像データのメモリへの書き込みまたは読み出しを行う。符号8は画像データ以外に、この画像データとセットになる撮影条件、日付、画像ファイル記号などの付随情報が記

録されるメモリである。符号9はCCDセンサからデータを取り出すためのタイミングパルス生成部(TG)、符号10はデジタルカメラ31のシステム全体の制御を行うシステムコントローラ、符号11はDRAMであり、画像データ処理を行うとき、このデータを一時的に保存するためのメモリである。

【0018】符号12はセキュリティ処理部であり、前記圧縮／伸張処理部6と連携してデータの改ざん防止処理を行う。符号13はキースイッチであり、デジタルカメラ31を立ちあげるための電源スイッチである。符号14はD/Aコンバータであり、画像データに基づきLCDをアクティブ化する。符号15は写真画像を表示する液晶表示器(LCD)16の表示器コントローラ(ENC)である。

【0019】次に、図1および図3によるデジタルカメラを使った写真システムのシステム図を参照して、この発明の一実施形態の動作を説明する。デジタルカメラ31で目的の写真を撮影し、このデジタルカメラ31のレンズ1を通して撮影された画像は、CCDイメージセンサ2に取り込まれ、補正処理部3において相関二重サンプリング、ガンマ補正、自動ホワイトバランスの各補正処理が行われた後、A/Dコンバータ4においてデジタル値に変換され、さらに、デジタル信号プロセッサ(DSP)5によって各ピクセルに対応したR、G、Bデータに変換される。

【0020】工事写真では撮影されたデータが撮影後に改ざんされては証拠写真としての信頼性に欠けるので改ざん防止の対策を講じるが、この改ざん防止の方式には2種類の方式がある。まず第1の方式は画像データが改ざんされた場合、改ざんされたことをチェックできる方式であり、この方式について以下に説明する。上述のDSP5によって各ピクセルに対応したR、G、Bデータに変換された信号は、圧縮／伸張処理部6において圧縮されたデータをさらに間引き、インデックス画像データを作成する。この場合単純な間引きより、原画像を大きな圧縮率で圧縮し、インデックス画像とする方が望ましい。

【0021】また、保存画像とこれに対応するインデックスとには1対1に対応するファイル記号がつけられ、常に一体のものとして扱われる。つまり、圧縮／伸張処理部6は画像データの圧縮、伸張の他、インデックス作成機能も合わせ持つ。メモリコントローラ7は、圧縮した画像およびインデックス画像データのメモリ8への書き込みと、このメモリ8からのデータの読み出しをコントロールする。

【0022】セキュリティ処理部12は前記インデックス画像に対して、電子印鑑と同様の原理により、一方向関数の逆関数を使って復号25鍵データによりセキュリティをかけて画像データを暗号化し、暗号化インデックスデータとする。このセキュリティをかけられた暗号化

インデックスデータは、一方向関数を使って、予め与えられている公開鍵データを用いることにより暗号化インデックスデータとして復元することができ、原インデックス画像データとの比較により、データ改ざんの有無を判定することができる。

【0023】上述の画像セキュリティシステムを備えたデジタルカメラから出力されるデータは次の5種類となり、図2(a)に示すように、電子記録メディアの電子ファイル20に、リレーションナルな画像データセット21として、次のようにセットで記録される。

- (1) 圧縮画像データ22
- (2) 画像に対応した個別情報データ23
- (3) 復号化キーでセキュリティのかけられた暗号化インデックスデータ24

【0024】また、前記セキュリティ処理部12の設定キーの中身は、数値あるいは計算式などのソフト的内容である。この設定キーが書き込まれるのは専用ICであり、書き込みデータの設定はハード的に固定され、外部からこの書き込みデータを知ることは不可能である。もし、無理に調べようすれば、ICそのものが破損し、使用不可能になるようになることができる。また、セキュリティの設定は、基本的には個々のカメラに固有の値を設定するが、固有の値でなく共通の値とすることもできる。

【0025】また、図2の画像ファイル20に書き込まれる情報のうち、公開鍵25、インデックス画像作成方法26は必ずしも画像電子ファイル20中に同時に書き込まれる必要はない、例えばファイルの名称を一括に書き込んだインデックスファイル中に書き込むといった別の手段によって書き込んでも良い。

【0026】これまでに説明してきたように、デジタルカメラからは画像データとセキュリティのかけられたインデックス画像が出力され、画像データはパソコンに取り込み画像の編集や画像の改ざんなどが自由に行えるが、セキュリティのかけられたインデックス画像は改ざんによりデータが破壊されてしまうので、改ざんは事実上不可能である。従って、写真画像が改ざんされたかどうかは、提出された写真画像と公開鍵を用いて復元したインデックス画像とを目視比較することによって改ざんされているかどうかをチェックすることができる。

【0027】また、人間の目に頼らなくても画像データから、インデックスを作成したときと同一の処理を行ってインデックス画像データを作成し、この作成したインデックス画像データと公開鍵を用いて復元したインデックス画像データとが一致するかどうかをパソコンなどを使って検証することが可能となる。

【0028】次に、データ改ざん防止の第2の方式について、上述の第1の方式と異なる部分について説明する。図1において、圧縮／伸張処理部6においてインデックスを作成せず、圧縮により作成された画像データそのものに復号鍵によって、セキュリティをかけ、メモリ7に格納する方式である。

【0029】この方式では、上述の画像セキュリティシステムを備えたデジタルカメラから出力されるデータは次の3種類となり、図2(b)に示すように、電子記録メディアの電子ファイル20に、リレーショナルな画像データセット21として、次のようにセットで記録される。

- (1) 暗号化して圧縮された暗号化圧縮画像データ27
- (2) 画像に対応した個別情報データ23

(3) セキュリティのかけられた暗号化圧縮画像データを復元するための公開鍵25

この方式は、画像データそのものを暗号化するため信頼度が高いが、上述の第1の方式に比べ、暗号化と復号化に要する演算処理時間が長くなる。

【0030】以上、本発明の一実施形態の動作を図面を参照して詳述してきたが、本発明はこの実施形態に限られるものではなく、本発明の要旨を逸脱しない範囲の設計変更等があっても本発明に含まれる。例えば、工事写真に限定せず、スキャナ、ビデオなどデジタル画像を扱い、かつセキュリティが問題となる全てのケースに適用できる。

### 【0031】

【発明の効果】これまでに説明したように、この発明の一実施形態の第1の方式によれば、画像データをサンプリングしたインデックス画像データに対して電子印鑑と同様の原理により、一方向関数の逆関数を使って復号鍵データによりセキュリティをかけ、画像データを暗号化し、このセキュリティをかけられた画像データは、一方で関数を使って、予め与えられている公開鍵データを用いることにより暗号化インデックスデータを復元するようにしたので、改ざんが行われた画像のチェックを行うことができるという効果が得られる。

【0032】さらに、この発明の一実施形態の第2の方式によれば、画像データそのものにセキュリティをかけ改ざん不能にすることができるという効果が得られる。

### 【図面の簡単な説明】

【図1】この発明の一実施形態による画像セキュリティシステムを備えたデジタルカメラの構成を示すブロッ

ク図である。

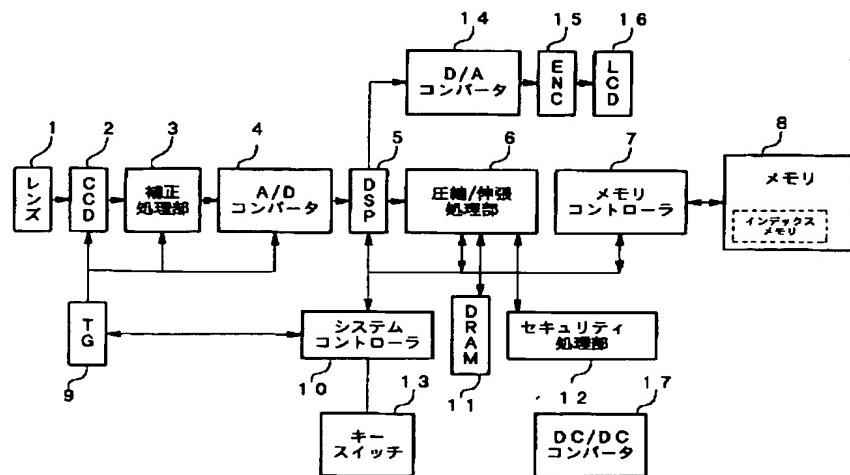
【図2】画像セキュリティシステムによる電子ファイル構造のイメージ図である。

【図3】デジタルカメラを使った写真システムを示す図である。

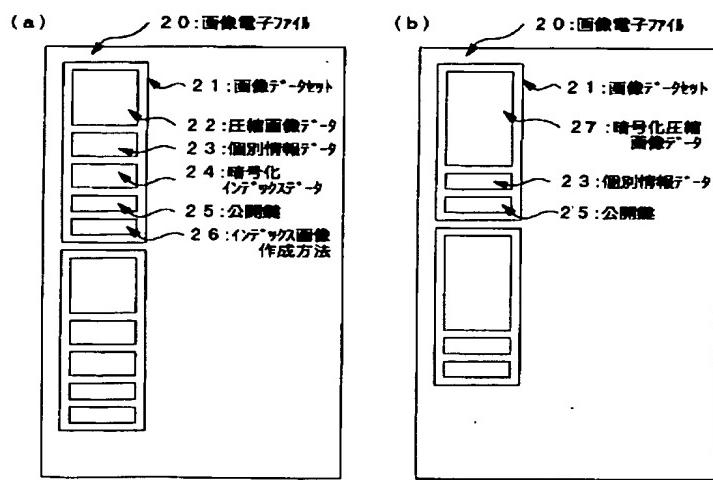
### 【符号の説明】

- |    |                  |
|----|------------------|
| 1  | レンズ              |
| 2  | CCDイメージセンサ(CCD)  |
| 3  | 補正処理部            |
| 4  | A/Dコンバータ         |
| 5  | デジタル信号プロセッサ(DSP) |
| 6  | 圧縮／伸張処理部         |
| 7  | メモリコントローラ        |
| 8  | メモリ              |
| 9  | タイミングパルス生成部(TG)  |
| 10 | システムコントローラ       |
| 11 | DRAM             |
| 12 | セキュリティ処理部        |
| 13 | キースイッチ           |
| 14 | D/Aコンバータ         |
| 15 | 表示器コントローラ(ENC)   |
| 16 | 液晶表示器LCD         |
| 17 | DC/DCコンバータ       |
| 20 | 画像電子ファイル         |
| 21 | 画像データセット         |
| 22 | 圧縮画像データ          |
| 23 | 個別情報データ          |
| 24 | 暗号化インデックスデータ     |
| 25 | 公開鍵              |
| 26 | インデックス画像作成方法     |
| 27 | 暗号化圧縮画像データ       |
| 31 | デジタルカメラ          |
| 32 | メモリカード挿入口        |
| 33 | インターフェース         |
| 34 | メモリカード           |
| 35 | PCカードリーダ         |
| 36 | インターフェース         |
| 37 | パソコン             |
| 38 | ディスプレイ           |
| 39 | カラープリンタ          |
| 40 | CDR              |
| 41 | アルバム編集ソフト        |

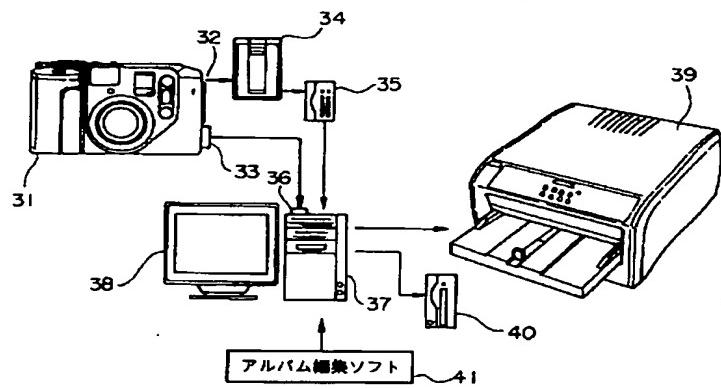
【図1】



【図2】



【図3】



---

フロントページの続き(51) Int.Cl.<sup>6</sup>

識別記号

F I

H 04N 5/91

H 04N 5/91

N